

Understanding the Rating Methodologies

Rating is a measurement of the degree of risk a given vulnerability poses to your business.

Note WhiteHat strongly recommends that customers utilize the Advanced Rating Methodology. This rating methodology allows sites and applications to be evaluated using the same standards, and reports based on the Advanced Rating Methodology will use the same rating scale for both sites and applications. In addition, the Advanced Rating Methodology allows customers to set [priorities](#) for their sites to assist in prioritizing the remediation of vulnerabilities according to business needs.

The Advanced Rating Methodology

In the Advanced Rating Methodology, sites and applications are evaluated in the same way: the rating is based on Risk.

Risk

Risk includes the following factors:

- **Likelihood:** How likely is it that a vulnerability will be exploited? This may be based on how widespread the knowledge of the vulnerability is, how easy it is to exploit, etc.
- **Impact:** how much damage may be done to your business if a vulnerability is exploited, as determined by the Threat Research Center.
- **Priority** (Sites only): How important this asset is to your business. You do not have to set a Priority for a site if you do not choose to; if no priority is set, priority will not be considered in the Risk calculations.

Risk is measured by the combination of the Likelihood and the Net Impact (based on Impact and Priority if any) associated with this vulnerability on this asset:


	Likelihood		
Net Impact	<i>Low Likelihood</i>	<i>Medium Likelihood</i>	<i>High Likelihood</i>
<i>Low Impact</i>	Risk: Note	Low Risk	Medium Risk
<i>Medium Impact</i>	Low Risk	Medium Risk	High Risk
<i>High Impact</i>	Medium Risk	High Risk	Critical Risk

In the Advanced Rating Methodology, all vulnerabilities are rated according to the Risk associated with the vulnerability for that asset (site or application). This will be reflected in the findings pages, in the dashboard, and in your reports.


The Legacy Rating Methodology

In the Legacy Rating Methodology, sites and applications are evaluated differently:

- Sites are rated according to *Severity*
- Applications are rated according to *Risk*. (See the information on Risk under the [Advanced Rating Methodology](#) description.)

 The Legacy Rating Methodology does not incorporate the site priority in its ratings.

Severity reflects the amount of damage that could be done to your business if a particular vulnerability is exploited. Severity is described as informational, low, medium, high, critical, or urgent. (An informational vulnerability reflects a situation where best practices may not be being followed, but no actual vulnerability is currently present.) In the Legacy Rating Methodology, vulnerabilities found on sites are rated according to the Severity of the vulnerability. This will be reflected in the findings pages, in the dashboard, and in your reports.

 In the Legacy Rating Methodology, the Rating shown in your reports and on your dashboard is based on Severity alone, but if you are viewing a particular vulnerability on the Vuln Details page, you can see the details under "Score." Score is a combination of Severity and Threat.

Threat levels are rated zero to five:

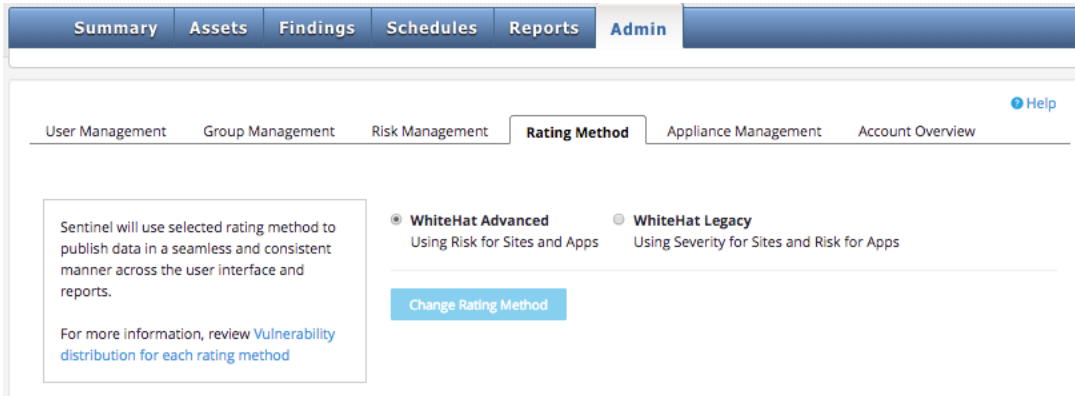
- 5 (Urgent): This is an easily exploited vulnerability; immediate remediation is recommended.
- 4 (Critical): This is a commonly exploited vulnerability; priority remediation is recommended.
- 3 (High): This is a regularly exploited vulnerability; priority remediation is recommended.
- 2 (Medium): This is a moderately difficult vulnerability to exploit. Remediation is recommended.
- 1 (Low): This is a difficult vulnerability to exploit. Remediation is recommended as possible.
- 0 (Informational): This is an informational finding with negligible risk. Remediation is recommended as best practice.

To change your rating methodology, please see "[Changing Your Rating Methodology](#)."

Changing Your Rating Methodology

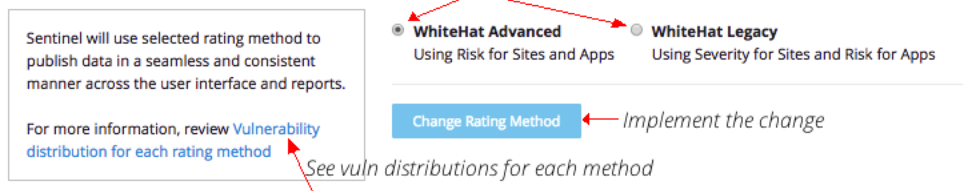
The rating method can be changed by the Sentinel Admin. Changes to the rating method will apply at the Client level – that is, all users will see data for all sites based on the rating method the Admin selects.

- Log into Sentinel.
- Click on the Admin tab and select the Rating Method sub-tab



- This will bring you to the Rating Method page:

Rating Method



If you would like to see how each rating method will affect your vulnerability distribution, click on the link for "review Vulnerability distribution for each rating method."

- Select the rating method you prefer, and click on the Change Rating Method button.

For more information on the two rating methods, please see [Managing Your Rating Methodology](#).

